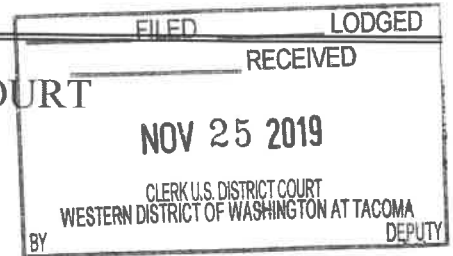


UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Information Associated with Apple ID Account:
christina.carpenter7@gmail.com that is Stored at the
Premises Controlled by Apple Inc.Case No. MJ19-5241

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 2251(a)	Attempted Production of Child Pornography
18 U.S.C. § 2252(a)(2)	Attempted Receipt/Distribution of Child Pornography
18 U.S.C. § 2422(b)	Attempted Enticement of a Minor

The application is based on these facts:

- ☒ See Affidavit of Special Agent Kyle McNeal, FBI, attached hereto and incorporated by reference herein.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.

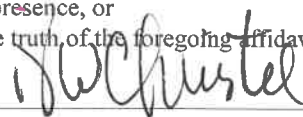


Applicant's signature

KYLE MCNEAL, Special Agent

Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 11/25/2019


Judge's signature

City and state: Tacoma, Washington

DAVID W. CHRISTEL, United States Magistrate Judge

Printed name and title

ATTACHMENT A
(Accounts to be Searched)

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with, the following Apple account (Target Account): Christina CARPENTER, Phone Number: (253) 722-7826, Apple ID: christina.carpenter7@gmail.com, as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B
(Particular Things to be Seized)

I. Information to be Disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the Target Account listed in Attachment A:

a. All records or other information regarding the identification of the Target Account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the Target Account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the Target Account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the Target Account, including stored or preserved copies of instant messages (including iMessages, SMS

1 messages; and MMS messages) sent to and from the Target Account (including all draft
2 and deleted messages), the source and destination account or phone number associated
3 with each instant message, the date and time at which each instant message was sent, the
4 size and length of each instant message, the actual IP addresses of the sender and the
recipient of each instant message, and the media, if any, attached to each instant message;

5 e. The contents of all files and other records stored on iCloud, including all
6 iOS device backups, all Apple and third-party app data, all files and other records related
7 to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud
8 Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud
Keychain, and all address books, contact and buddy lists, notes, reminders, calendar
entries, images, videos, voicemails, device settings, and bookmarks;

9 f. All activity, connection, and transactional logs for the Target Account (with
10 associated IP addresses including source port numbers), including FaceTime call
11 invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including
12 purchases, downloads, and updates of Apple and third-party apps), messaging logs
13 (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on
14 logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with
iOS device activation and upgrades, and logs associated with web-based access of Apple
services (including all associated identifiers);

15 g. All records and information regarding locations where the account was
16 accessed, including all data stored in connection with Location Services;

17 h. All records pertaining to the types of service used;

18 i. All records pertaining to communications between Apple and any person
19 regarding the account, including contacts with support services and records of actions
20 taken; and

21 j. All files, keys, or other information necessary to decrypt any data produced
22 in an encrypted form, when available to Apple (including, but not limited to, the
keybag.txt and fileinfolist.txt files).

23
24 **The Provider is hereby ordered to disclose the above information to the
government within 14 days of service of this warrant.**

25
26 **II. Information to be Seized by the Government**

27 All information described above in Section I that constitutes fruits, evidence
28 and/or instrumentalities of violations of 18 U.S.C. § 2251(a) (Attempted Production of

1 Child Pornography), 18 U.S.C. § 2252(a)(2) (Attempted Receipt/Distribution of Child
2 Pornography), and 18 U.S.C. § 2422(b) (Attempted Enticement of a Minor), involving
3 Jonathan David CARPENTER, these violations having occurred between on or about
4 September 9, 2018, and September 10, 2018, including, for the Target Account listed on
5 Attachment A, evidence retained in the Target Account from August 1, 2018, to
6 September 30, 2018, including the following matters:

7 a. Evidence that serves to identify any person who has used or accessed the
8 Target Account or who has exercised in any way any dominion or control over the Target
9 Account;

10 b. Evidence that may reveal the current or past location of the individual or
11 individuals using the Target Account;

12 c. Evidence indicating how and when the account was accessed or used, to
13 determine the chronological and geographic context of account access, use and events
14 relating to the crime under investigation and the Target Account subscriber;

15 d. Any records pertaining to the means and source of payment for Apple
16 services (including any credit card or bank account number or digital money transfer
17 account information);

18 e. Evidence indicating the Target Account user's state of mind as it relates to
19 the aforementioned crimes under investigation;

20 f. Communications between the Target Account and any minors regarding the
21 above-referenced offenses;

22 g. All records or other information regarding the devices associated with, or
23 used in connection with, the account (including all current and past trusted or authorized
24 iOS devices and computers, and any devices used to access Apple services), including
25 serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"),
26 Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses,
27 Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"),
28 Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"),
Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile
Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International
Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment
Identities ("IMEI");

1 h. All records and information regarding locations where the Target Account
2 was accessed, including all data stored in connection with Location Services;

3 i. Subscriber records associated with the Target Account, including 1) names,
4 email addresses, and screen names; 2) physical addresses; 3) records of session times and
5 durations; 4) length of service (including start date) and types of services utilized;
6 5) telephone or instrument number or other subscriber number or identity, including any
7 temporarily assigned network address such as IP address, media access card addresses, or
8 any other unique device identifiers recorded by internet service provider in relation to the
9 account; 6) account log files (login IP address, account activation IP addresses, and IP
10 address history); 7) detailed billing records/logs; 8) means and source of payment; and 9)
11 lists of all related accounts;

12 j. Records of communications between the Apple and any person purporting
13 to be the account holder of the Target Account about issues relating to the Target
14 Account, such as technical problems, billing inquiries, or complaints from other users
15 about the specified account. This to include records of contacts between the subscriber
16 and the provider's support services, as well as records of any actions taken by the
17 provider or subscriber as a result of the communications;

18 k. Information identifying accounts that are linked or associated with the
19 Target Account;

20 l. Any visual depiction of minor(s) engaged in sexually explicit conduct, in
21 any format or media; and

22 m. All messages, documents and profile information, attachments, or other
23 data that otherwise constitutes evidence, fruits, or instrumentalities of violations of 18
24 U.S.C. §§ 2252(a)(2)(Receipt and Distribution of Child Pornography) and
25 2252(a)(4)(Possession of Child Pornography).

26
27 **Notwithstanding the criminal offenses defined under 18 U.S.C. § 2252 and 2252A or**
28 **any similar criminal offense, Apple shall disclose information responsive to this**
warrant by mailing it to the Federal Bureau of Investigation, Attn: Kyle McNeal at
the Tacoma Resident Agency, Seattle Division, or via email to kmcneal@fbi.gov.

[illegible]

I. INTRODUCTION AND AGENT BACKGROUND

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), assigned to the Special Agent in Charge in Seattle, Washington. I have been an Agent with the FBI since April 2011. My training at the FBI Academy in Quantico, Virginia, included courses in law enforcement techniques, federal criminal statutes, conducting complex criminal investigations, physical and electronic surveillance techniques, and the execution of search warrants. During my employment as a law enforcement officer, I have attended periodic seminars, meetings, and continued training.

3. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code §§ 2251(a), 2252(a)(2), and 2422(b). I have received training in the area of child pornography and child exploitation, and have observed and reviewed numerous examples of child pornography in various forms of media, including media stored on digital media storage devices such as computers, tablets, cellphones, etc. I have also participated in the execution of numerous search warrants involving investigations of child exploitation and/or child pornography offenses. I work with other federal, state, and local law enforcement personnel in the investigation and prosecution of crimes involving the sexual exploitation of children.

4. The facts in this affidavit come from my training, experience, and information obtained from other agents and witnesses. I have not included every fact known concerning this investigation. I have set forth the facts that I believe are necessary for a fair determination of probable cause for the requested search warrants.

II. PURPOSE OF AFFIDAVIT

5. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), and Rule 41 of the Federal Rules of Criminal Procedure, for information associated with the following Apple account: Christina CARPENTER, Phone Number: (253) 722-7826, Apple ID: christina.carpenter7@gmail.com (“Target Account”), which is further described in Attachment A (attached hereto and incorporated by reference as if fully set forth herein), for evidence, fruits and instrumentalities, as further described in Attachment B (attached hereto and incorporated by reference as if fully set forth herein), of the crimes of 18 U.S.C. § 2251(a) (Attempted Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Attempted Receipt/Distribution of Child Pornography), and 18 U.S.C. § 2422(b) (Attempted Enticement of a Minor):

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. §§ 2711, 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A). Specifically, the Court is “in a district court of the United States... that – has jurisdiction over the offense[s] being investigated.” 18 U.S.C. § 2711(3)(A)(i).

7. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

III. SOURCES OF INFORMATION

8. I have obtained the facts set forth in this affidavit from oral and written reports of other law enforcement officers as well as from records, documents and other evidence obtained during this investigation. I have reviewed official reports prepared by other law enforcement officers participating in this investigation and in the other related investigations by agencies referenced in this affidavit.

IV. TECHNICAL TERMS AND BACKGROUND

9. Based on my training and experience, and information from other experienced agents, I use the following technical terms to convey the following meanings:

a. “Internet Service Providers” (ISPs) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

b. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet.

c. “Domain names” are common, easy to remember names associated with an IP address. For example, a domain name of “www.usdoj.gov” refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delineated by a period.

d. “Website” consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

e. A “Preservation Letter” is a letter governmental entities may issue to Internet providers pursuant to 18 U.S.C. § 2703(f) to ensure that the Internet Providers preserve records in its possession. The preservation of such records is necessary given the dynamic nature of digital records that may be deleted. As is the case with most

1 digital technology, communications by way of computer can be saved or stored on the
2 computer used for these purposes. Storing this information can be intentional, i.e., by
3 saving an email as a file on the computer or saving the location of one's favorite websites
4 in, for example, "bookmarked" files. Digital information can also be retained
5 unintentionally, e.g., traces of the path of an electronic communication may be
6 automatically stored in many places (e.g., temporary files or ISP client software, among
7 others). In addition to electronic communications, a computer user's Internet activities
8 generally leave traces or "footprints" in the web cache and history files of the browser
9 used. A forensic examiner often can recover evidence suggesting whether a computer
10 contains peer to peer software, when the computer was sharing files, and some of the files
11 which were uploaded or downloaded. Such information is often maintained indefinitely
12 until overwritten by other data.

13 f. **Email and Data Storage:** In general, an email that is sent to a
14 subscriber of the service provider is stored in the subscriber's "in-box" on the service
15 provider's servers until the subscriber deletes the email. If the subscriber does not delete
16 the message, the message can remain on service provider's servers indefinitely. The user
17 can move and store messages in personal folders such as a "sent folder." In recent years,
18 the service provider and other ISPs have provided their users with larger storage
19 capabilities associated with their users' email account. ISPs, including the service
20 provider, provide users with as much as multiple gigabytes of online storage space.
21 Based on my experience and conversations with other law enforcement officers with
22 experience in executing and reviewing search warrants of email accounts, I have learned
23 that search warrants for email accounts and computer systems have revealed stored
24 emails sent and/or received many years prior to the date of the search. The service
25 provider also provides subscribers with various other associated products and services in
26 connection with their accounts, including chat programs, photo and video sharing
27 platforms and other services or social media programs.
28

1 g. **Data Retention:** When the subscriber sends an email, it is initiated
2 at the user's computer or other internet access device, transferred via the Internet to the
3 service provider's servers, and then transmitted to its end destination. The service
4 provider often saves a copy of the email sent. Unless the sender of the email specifically
5 deletes the email from the service provider's servers, the email can remain on the system
6 indefinitely.

7 h. **Email Messages:** A sent or received email typically includes the
8 content of the message, source and destination addresses, the date and time at which the
9 email was sent, and the size and length of the email. If an email user writes a draft
10 message but does not send it, that message may also be saved by the service provider but
11 may not include all of these categories of data.

12 i. **Online Data Storage:** A subscriber of the service provider can also
13 store files, including emails, address books, contact or buddy lists, calendar data, pictures,
14 and other files on servers maintained and/or owned by the service provider. Subscribers
15 to the service provider might not store on their home computers copies of the emails
16 stored in the Target Account. This is particularly true when they access the Target
17 Account through the web, or if they do not wish to maintain particular emails or files in
18 their residence. In essence, a subscriber's email box has become a common online data
19 storage location for many users. This is particularly true when they access the Target
20 Account through the web, or if they do not wish to maintain particular emails or files in
21 their residence.

22 j. **Identifying Information:** In general, email providers such as the
23 service provider ask each of their subscribers to provide certain personal identifying
24 information when registering for an email account. This information could include the
25 subscriber's full name, physical address, telephone numbers and other identifiers, such as
26 alternative email addresses, and, for paying subscribers, means and source of payment
27 (including any credit or bank account number).
28

1 k. **Transactional Information:** Service providers typically retain
 2 certain transaction information about the creation and use of each account on their
 3 systems. This information can include the date on which the account was created, the
 4 length of service, records of log-in (i.e., session) times and durations, the types of service
 5 utilized, the status of the account (including whether the account is inactive or closed),
 6 the methods used to connect to the account (such as logging into the account via service
 7 provider's website), and other log files that reflect usage of the account. In addition,
 8 email providers often have records of the IP address used to register the account and the
 9 IP addresses associated with particular logins to the account. Because every device that
 10 connects to the Internet must use an IP address, IP address information can help to
 11 identify which computers or other devices were used to access the email account.

12 l. **Technical Support:** In some cases, account users will communicate
 13 directly with a service provider about issues relating to the account, such as technical
 14 problems, billing inquiries, or complaints from other users. Service providers typically
 15 retain records about such communications, including records of contacts between the user
 16 and the providers support services, as well as records of any actions taken by the provider
 17 or user as a result of the communications.

18 m. **Attribution Evidence:** In my training and experience, evidence of
 19 who was using an account may be found in address books, calendars, contact or buddy
 20 lists, emails in the account, and attachments to emails, including pictures and files.

21 10. The assigned number to a cellular telephone (known as the mobile directory
 22 number or MDN), and the identifying telephone serial number (Electronic Serial
 23 Number, or ESN), (Mobile Identification Number, or MIN), (International Mobile
 24 Subscriber Identity, or IMSI), or (International Mobile Equipment Identity, or IMEI) are
 25 important evidence because they reveal the service provider, allow us to obtain subscriber
 26 information, and uniquely identify the telephone. This information can be used to obtain
 27 toll records, to identify contacts by this telephone with other cellular telephones, and to
 28 identify other telephones used by the same subscriber or purchased as part of a package.

1 11. The stored list of recent received calls and sent calls is important evidence.
2 It identifies telephones recently in contact with the telephone user. This is valuable
3 information in a child pornography case because it will identify telephones used by minor
4 victims. Stored text messages and stored emails may also reveal important evidence.

5 12. Photographs on a cellular telephone are evidence because they help identify
6 the user, either through his or her own picture, or through pictures of friends, family, and
7 associates that can identify the user.

8 13. Based on my training and experience, and my discussions with other
9 experienced officers and agents involved in investigations, as well as information
10 published by Apple on its website,¹ I know the following information regarding the
11 iCloud and Apple IDs:

12 a. Apple is a United States company that produces the iPhone, iPad,
13 and iPod Touch, all of which use the iOS operating system, and desktop and laptop
14 computers based on the Mac OS operating system.

15 b. Apple provides a variety of services that can be accessed from Apple
16 devices or, in some cases, other devices via web browsers or mobile and desktop
17 applications (“apps”). As described in further detail below, the services include email,
18 instant messaging, and file storage.

19 c. Apple provides email service to its users through email addresses at
20 the domain names mac.com, me.com, and icloud.com.

21 d. iMessage and FaceTime allow users of Apple devices to
22 communicate in real-time. iMessage enables users of Apple devices to exchange instant
23

24 ¹ This information includes, but is not limited to, the following document and webpages: “U.S.
25 Law Enforcement Legal Process Guidelines,” available at:
26 <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an
27 Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at
28 <http://www.apple.com/icloud/>; “iCloud: iCloud storage and backup overview,” available at
<https://support.apple.com/kb/PH12519>; and “iOS Security,” available at
https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf.

1 messages (“iMessages”) containing text, photos, videos, locations, and contacts, while
2 FaceTime enables those users to conduct video calls.

3 e. iCloud is a file hosting, storage, and sharing service provided by
4 Apple. iCloud can be utilized through numerous iCloud-connected services, and can also
5 be used to store iOS device backups and data associated with third-party apps.

6 f. iCloud-connected services allow users to create, store, access, share,
7 and synchronize data on Apple devices or via icloud.com on any Internet-connected
8 device. For example, iCloud Mail enables a user to access Apple-provided email
9 accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My
10 Photo Stream can be used to store and manage images and videos taken from Apple
11 devices, and iCloud Photo Sharing allows the user to share those images and videos with
12 other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets,
13 and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages
14 opened in the Safari web browsers on all of the user’s Apple devices. iWorks Apps, a
15 suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to
16 create, store, and share documents, spreadsheets, and presentations. iCloud Keychain
17 enables a user to keep website username and passwords, credit card information, and
18 Wi-Fi network information synchronized across multiple Apple devices.

19 g. The “Game Center,” Apple’s social gaming network, allows users of
20 Apple devices to play and share games with each other.

21 h. “Find My iPhone” allows owners of Apple devices to remotely
22 identify and track the location of, display a message on, and wipe the contents of those
23 devices.

24 i. Location Services allows apps and websites to use information from
25 cellular, Wi-Fi, Global Positioning System (“GPS”) networks, and Bluetooth, to
26 determine a user’s approximate location.

27 j. The “App Store” and “iTunes Store” are used to purchase and
28 download digital content. iOS apps can be purchased and downloaded through the “App

1 Store” on iOS devices, or through the “iTunes Store” on desktop and laptop computers
2 running either Microsoft Windows or Mac OS. Additional digital content, including
3 music, movies, and television shows, can be purchased through the “iTunes Store” on
4 iOS devices and on desktop and laptop computers running either Microsoft Windows or
5 Mac OS.

6 k. Apple services are accessed through the use of an “Apple ID,” an
7 account created during the setup of an Apple device or through the iTunes or iCloud
8 services. A single Apple ID can be linked to multiple Apple services and devices,
9 serving as a central authentication and syncing mechanism.

10 l. An Apple ID takes the form of the full email address submitted by
11 the user to create the account; it can later be changed. Users can submit an Apple-
12 provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an
13 email address associated with a third-party email provider (such as Gmail, Yahoo, or
14 Hotmail). The Apple ID can be used to access most Apple services (including iCloud,
15 iMessage, and FaceTime) only after the user accesses and responds to a “verification
16 email” sent by Apple to that “primary” email address. Additional email addresses
17 (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an
18 Apple ID by the user.

19 m. Apple captures information associated with the creation and use of
20 an Apple ID. During the creation of an Apple ID, the user must provide basic personal
21 information including the user’s full name, physical address, and telephone numbers.
22 The user may also provide means of payment for products offered by Apple. The
23 subscriber information and password associated with an Apple ID can be changed by the
24 user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition,
25 Apple captures the date on which the account was created, the length of service, records
26 of log-in times and durations, the types of service utilized, the status of the account
27 (including whether the account is inactive or closed), the methods used to connect to and
28

1 utilize the account, the Internet Protocol address (“IP address”) used to register and
2 access the account, and other log files that reflect usage of the account.

3 n. Additional information is captured by Apple in connection with the
4 use of an Apple ID to access certain services. For example, Apple maintains connection
5 logs with IP addresses that reflect a user’s sign-on activity for Apple services such as
6 iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot
7 pages on Apple’s website. Apple also maintains records reflecting a user’s app purchases
8 from App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail
9 logs” for activity over an Apple-provided email account. Records relating to the use of
10 the Find My iPhone service, including connection logs and requests to remotely lock or
11 erase a device, are also maintained by Apple.

12 o. Apple also maintains information about the devices associated with
13 an Apple ID. When a user activates or upgrades an iOS device, Apple captures and
14 retains the user’s IP address and identifiers such as the Integrated Circuit Card ID number
15 (“ICCID”), which is the serial number of the device’s SIM card. Similarly, the telephone
16 number of a user’s iPhone is linked to an Apple ID when the user signs in to FaceTime or
17 iMessage. Apple also may maintain records of other device identifiers, including the
18 Media Access Control address (“MAC address”), the unique device identifier (“UDID”),
19 and the serial number. In addition, information about a user’s computer is captured when
20 iTunes is used on that computer to play content associated with an Apple ID, and
21 information about a user’s web browser may be captured when used to access services
22 through icloud.com and apple.com. Apple also retains records related to communications
23 between users and Apple customer service, including communications regarding a
24 particular Apple device or service, and the repair history for a device.

25 p. Apple provides users with five gigabytes of free electronic space on
26 iCloud, and users can purchase additional storage space. That storage space, located on
27 servers controlled by Apple, may contain data associated with the use of iCloud-
28 connected services, including: email (iCloud Mail); images and videos (iCloud Photo

1 Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets,
2 presentations, and other files (iWorks and iCloud Drive); and web browser settings and
3 Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used
4 to store iOS device backups, which can contain a user's photos and videos, iMessages,
5 Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages,
6 voicemail messages, call history, contacts, calendar events, reminders, notes, app data
7 and settings, and other data. Records and data associated with third-party apps may also
8 be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging
9 service, can be configured to regularly back up a user's instant messages on iCloud.
10 Some of this data is stored on Apple's servers in an encrypted form but can nonetheless
11 be decrypted by Apple.

12 q. In my training and experience, evidence of who was using an Apple
13 ID and from where, and evidence related to criminal activity of the kind described above,
14 may be found in the files and records described above. This evidence may establish the
15 "who, what, why, when, where, and how" of the criminal conduct under investigation,
16 thus enabling the United States to establish and prove each element or, alternatively, to
17 exclude the innocent from further suspicion.

18 r. For example, the stored communications and files connected to an
19 Apple ID may provide direct evidence of the offenses under investigation. Based on my
20 training and experience, instant messages, emails, voicemails, photos, videos, and
21 documents are often created and used in furtherance of criminal activity, including to
22 communicate and facilitate the offenses under investigation.

23 s. In addition, the user's account activity, logs, stored electronic
24 communications, and other data retained by Apple can indicate who has used or
25 controlled the account. This "user attribution" evidence is analogous to the search for
26 "indicia of occupancy" while executing a search warrant at a residence. For example,
27 subscriber information, email and messaging logs, documents, and photos and videos
28 (and the data associated with the foregoing, such as geo-location, date and time) may be

1 evidence of who used or controlled the account at a relevant time. As an example,
2 because every device has unique hardware and software identifiers, and because every
3 device that connects to the Internet must use an IP address, IP address and device
4 identifier information can help to identify which computers or other devices were used to
5 access the account. Such information also allows investigators to understand the
6 geographic and chronological context of access, use, and events relating to the crime
7 under investigation.

8 t. Account activity may also provide relevant insight into the account
9 owner's state of mind as it relates to the offenses under investigation. For example,
10 information on the account may indicate the owner's motive and intent to commit a crime
11 (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g.,
12 deleting account information in an effort to conceal evidence from law enforcement).

13 u. Other information connected to an Apple ID may lead to the
14 discovery of additional evidence. For example, the identification of apps downloaded
15 from App Store and iTunes Store may reveal services used in furtherance of the crimes
16 under investigation (e.g., a list of apps might reveal banking institutions used by these
17 individuals and lead to evidence of money laundering) or services used to communicate
18 with co-conspirators, such as sources of supply or redistributors. In addition, emails,
19 instant messages, Internet activity, documents, and contact and calendar information can
20 lead to the identification of co-conspirators and instrumentalities of the crimes under
21 investigation.

22 v. Therefore, Apple's servers are likely to contain stored electronic
23 communications and information concerning subscribers and their use of Apple's
24 services. In my training and experience, such information may constitute evidence of the
25 crimes under investigation including information that can be used to identify the
26 account's user or users.

V. PROBABLE CAUSE

14. Minor Victim 1 is a 13-year-old boy born in April 2006. Minor Victim 2 is a 12-year-old boy born in July 2007. On September 17, 2018, MV1 and MV2's mother, Christina Carpenter, notified U.S. Army CID special agents of her concerns that JONATHAN DAVID CARPENTER had sexually abused MV1 and MV2 (she also notified agents that MV2 suffered from autism). The allegations in this case include offenses occurring during three separate time intervals in three different geographical locations including: (1) in 2013, CARPENTER allegedly sexually abused MV1 while the family lived near Fort Drum in upstate New York; (2) in the fall of 2015, CARPENTER allegedly committed the offenses of Aggravated Sexual Abuse of a Child under 12 against MV1 and MV2 in violation of 18 U.S.C. §§ 2241(c), 2246(2) and 7 while the family resided on Joint Base Lewis-McChord; and (3) on or about September 10, 2018, CARPENTER allegedly used MV1's iPhone 7 to solicit nude images from approximately three of MV1's minor friends while residing in Lacey, Washington, in violation of 18 U.S.C. §§ 2251(a) and (e), 2252(a)(2) and 2422(b) and (2).

15. The information associated with the **Target Account**, which is further described in Attachment A, for the evidence, fruits and instrumentalities, as further described in Attachment B of the previously enumerated offenses is primarily tethered to the third category of offenses.

16. On September 26, 2018, CARPENTER was indicted for the offenses of aggravated sexual abuse of a child under the age of 12 against MV1 and MV2 arising from the instant allegations in violation of 18 U.S.C. §§ 2241(c), 2246(2) and 7. On September 25, 2019, CARPENTER was charged by way of a superseding indictment for one additional offense of attempted production of child pornography in violation of 18 U.S.C. §§ 2251(a) and (e).

17. On the afternoon of September 17, 2018, interviews were conducted with MV1 and MV2. Based upon the victims' allegations and their cohabitation with CARPENTER, agents conducted a probable cause arrest.

1 18. On September 17, 2018, CID Special Agent (SA) Dan Chandler conducted
2 a forensic interview of MV1. MV1 stated that when he was approximately seven years
3 old, his mother, Christina Carpenter left their residence for a period of approximately 11
4 days. It is believed that this occurred in 2013 when MV1 was in the 2nd Grade at
5 Knickerbocker Elementary School. The family was residing in Watertown, New York,
6 during this time.

7 19. MV1 recalled that he awoke one night and needed to use the restroom.
8 MV1 stated that, while disoriented, he stumbled into the living room, mistakenly believed
9 he had reached the restroom and began to urinate on the floor.

10 20. Meanwhile, CARPENTER was naked on the couch watching the television
11 show "Archer." MV1 stated that CARPENTER became angry, placed a rag into MV1's
12 mouth, and bent MV1 over. MV1 stated that CARPENTER then anally penetrated him
13 with his penis. At one point, the rag fell out of his mouth, which CARPENTER replaced.
14 MV1 stated that CARPENTER continued to penetrate him for an unknown amount of
15 time. When the attack ended, MV1 fled to his room crying and did not recall whether
16 CARPENTER ejaculated or wore a condom.

17 21. MV1 stated that a second incident occurred during the same 11-day period
18 in New York when Christina Carpenter was absent from the residence. MV1 recalled
19 that CARPENTER was again laying on the couch in the nude and called MV1 to him.
20 MV1 stated that CARPENTER then performed oral sex on MV1. CARPENTER then
21 told MV1 "Okay, it's your turn," to which MV1 responded "no."

22 22. MV1 stated that a third incident may have occurred during the same 11-day
23 period when Christina Carpenter was away from the home. MV1 alleged that
24 CARPENTER directed him to sleep in CARPENTER's bed, which MV1 did. MV1
25 awoke some time later after his clothes had been removed. MV1 did not recall how this
26 had happened.

27 23. MV1 stated that sometime in 2015, while watching television at the
28 Montgomery Street residence on JBLM, CARPENTER told MV1 to play cards with him.

1 MV1 remembered that CARPENTER told him they would “play like a casino, except
2 instead of chips we use clothes.”

3 24. MV1 claimed that he and CARPENTER ultimately disrobed while playing
4 the Defendant’s game. CARPENTER then directed MV1 to go to CARPENTER’s room
5 and lay down. MV1 complied. CARPENTER then entered the room and penetrated
6 MV1’s anus. MV1 stated that he believed CARPENTER used his finger although MV1
7 conceded that he only felt, but did not observe, the penetration. MV1 stated that
8 CARPENTER then rolled him onto his back and told MV1 to “suck his dick,” to which
9 MV1 replied “no” and fled the room. MV1 stated that he disclosed some of the details to
10 Christina Carpenter when she returned home.

11 25. On September 17, 2018, CID agents interviewed Christina Carpenter.
12 Christina Carpenter told agents that sometime between August and October of 2015,
13 MV1 had disclosed that CARPENTER digitally penetrated MV1’s anus with
14 CARPENTER’s finger. Christina Carpenter stated that this disclosure occurred while
15 they were living at their on-post residence located on Montgomery Street, JBLM,
16 Washington 98433.

17 26. On August 27, 2019, agents re-interviewed Christina Carpenter. Christina
18 now recalled that the incident with MV1 likely took place in approximately June or July
19 2015 when she was away from the family residence undergoing a sleep study. Christina
20 recalls that the family lived in the JBLM residence from May 2015 through December
21 31, 2015.

22 27. The morning following the sleep study, she received a peculiar voice-mail
23 from CARPENTER in which he claimed MV1 had falsely accused him of inappropriately
24 touching him and specifically alleged: “[MV1] is lying, I never touched him.” Christina
25 later called CARPENTER and his story changed. CARPENTER now claimed that he
26 was taking MV1 into his bedroom to apply lotion to MV1’s buttocks to treat a sunburn.
27 CARPENTER insisted that he did not digitally penetrate MV1’s anus. When asked why
28 he took MV1 to the bedroom for the lotion application, CARPENTER told Christina

1 Carpenter “I don’t know, I just did.” Christina Carpenter did not know if CARPENTER
2 actually applied the lotion on MV1’s buttocks, but MV1 told her that he did.

3 28. When Christina Carpenter returned to the residence, MV1 was very upset,
4 “in tears,” and claimed CARPENTER had digitally penetrated his anus. Christina
5 Carpenter checked MV1’s posterior for a sunburn and only saw that his back was “a little
6 red” but his buttocks did not display similar discoloration. However, because Christina
7 Carpenter did not observe any evidence of acute anal injury/redness, she made what she
8 now characterizes as a “horrible judgment call” by assuming MV1 had made a false
9 accusation. Christina Carpenter reasoned that she did not believe MV1 at the time
10 because she was triggered by her own sexual trauma that she had previously suffered
11 while deployed to Korea. She was “scared” and did not originally want to believe MV1
12 but now regrets this decision.

13 29. Christina Carpenter acknowledges MV1 has never manufactured any other
14 sexual misconduct allegations concerning CARPENTER or anyone else. The only acts
15 of dishonesty that she could identify were MV1’s occasional failures to take
16 responsibility for minor juvenile acts.

17 30. Following this incident, Christina Carpenter observed that MV1 was
18 increasingly reluctant to spend time with CARPENTER. Christina Carpenter did recall
19 traveling away from New York for an Army field exercise in approximately March 2013
20 or 2014 that could have lasted 11 days.

21 31. Christina Carpenter also corroborated that she and CARPENTER enforced
22 a policy that MV1 was required to turn-in his iPhone 7 every Friday and Saturday night at
23 approximately 10 p.m. (9 p.m. on weeknights). She also knew that MV1 had retained
24 the iPhone 4 but did not know that he retained access to Instagram by connecting through
25 the family’s WiFi.

26 32. Christina Carpenter acknowledged CARPENTER also consumed
27 significant amounts of alcohol. Once they relocated to JBLM in 2015, CARPENTER
28 increased his drinking frequency by consuming at least three mixed beverages each night.

1 When heavily intoxicated, Christina Carpenter observed CARPENTER wandering
2 through their home while nude (more than once per month on average).

3 33. On September 17, 2018, MV2 was interviewed by Susan Villa, Child
4 Forensic Interviewer, at Monarch Children's Justice Center in Lacey, Washington.
5 During the child forensic interview, MV2 provided the following details of his interaction
6 with CARPENTER in CARPENTER's bedroom of the JBLM Montgomery Street duplex
7 in which the family lived.

8 34. MV2 stated that the following incidents occurred while at "the duplex,"
9 which Christina Carpenter identified as 8431 Montgomery Street, JBLM, Washington.
10 MV2 estimated that the incident occurred about three years prior to the interview with
11 Villa, when MV2 was in 3rd grade (MV2 was enrolled in the 3rd Grade during the 2015-
12 2016 school year).

13 35. MV2 stated that CARPENTER sent MV2 to CARPENTER's room. MV2
14 stated that while in CARPENTER's room, CARPENTER told MV2 to "suck
15 [CARPENTER's] 'pee-pee,'" to which MV2 replied "No, am I gay?" and "Are you
16 gay?" MV2 claimed that CARPENTER said "just do it," to which MV2 asked "What
17 happens if I don't?" MV2 stated that CARPENTER replied "I'll spank you." MV2
18 stated that he was sitting on the bed and CARPENTER was standing near the bed. MV2
19 stated that CARPENTER pulled down CARPENTER's pants. MV2 disclosed that he
20 then "sucked [CARPENTER's] 'pee-pee'" and that "pee went out in my mouth." MV2
21 stated that he "spit it out" in the bathroom, but on another occasion, CARPENTER
22 wanted MV2 to "swallow it."

23 36. MV2 described an incident that occurred at the "duplex" where
24 CARPENTER "humped" MV2. It is believed that this took place in approximately 2015.
25 MV2 described the incident taking place in CARPENTER's bedroom while they were
26 both nude. MV2 was laying on the bed while CARPENTER "put his "pee pee" in
27 [MV2's] butt." CARPENTER was also spanking MV2 during this incident.
28

1 37. On August 27, 2019, an FBI Forensic Interviewer recorded a second
2 interview of MV2. MV2 remembered that CARPENTER humped and spanked MV2 in
3 “the duplex” on JBLM. CARPENTER had removed MV2’s clothes before assaulting
4 him. CARPENTER physically forced MV2’s mouth onto his penis. MV2 also disclosed
5 that CARPENTER told MV2 that “he would kill” him if MV2 told anyone about the
6 abuse. Based MV2 responses, it was unknown when or during what instance
7 CARPENTER made this threat.

8 38. MV2 largely restated his prior allegations with a couple of notable
9 exceptions. MV2 claimed that he only placed his mouth on CARPENTER’s penis once,
10 not twice. During this latter interview, MV2 could not recall his age at the time or the
11 academic year during which the abuse took place.

12 39. Agents did acknowledge that, during the forensic interviews, MV2
13 presented apparent difficulty with expressing chronological explanations of all incidents,
14 including descriptions of events not related to the reported offenses. MV2 spoke in
15 disjointed sentences throughout and required multiple questions to clarify details about
16 incidents, including locations of incidents, when incidents occurred, and differentiating
17 two incidents of described oral penetration and two incidents of “humping.” Specifically,
18 MV2 required multiple questions to differentiate two incidents of “humping,” one in
19 which CARPENTER was allegedly wearing shorts and one in which CARPENTER was
20 nude.

21 40. With the exception of the clothed “humping” disclosure, the alleged
22 incidents occurred at an on-post JBLM residence that is located within the special
23 maritime and territorial jurisdiction of the United States and the Western District of
24 Washington.

25 41. During his interview, MV1 described an incident that occurred between
26 CARPENTER and MV2 at their residence on JBLM in approximately 2015. MV2 got in
27 trouble at school. When MV2 returned home, CARPENTER told MV2 to go to
28 CARPENTER’s room. MV1 stated that he did not see what happened in the room, but

1 questioned MV2 after the incident took place. MV2 disclosed that CARPENTER
2 spanked him with CARPENTER's "pee pee." Additional disclosures were made by
3 MV2 to MV1 in 2018 regarding the sexual abuse of MV2 by CARPENTER. In 2018,
4 MV2 disclosed to MV1 that CARPENTER forced MV2 to "suck his dick." This incident
5 is also believed to have occurred on JBLM in 2015.

6 42. During her September 17, 2018, interview, Christina Carpenter informed
7 agents that MV2 disclosed to her that CARPENTER "made him suck his 'pee-pee' until
8 pee came out." Christina Carpenter stated that she did not ask any follow-up questions
9 but instead told CARPENTER she wanted to seek counseling for the children without
10 him present.

11 43. MV1 stated that approximately one week prior to his interview, on or about
12 September 9, 2018, MV1 provided his iPhone 7 to CARPENTER at approximately 10:00
13 PM, pursuant to the family's cell phone rule. It is believed that this event occurred
14 during the first night that Christina Carpenter was absent from the home on a weeklong
15 work-trip outside of the state. MV1 stated that he also had an iPhone 4 in his bedroom of
16 which CARPENTER was unaware. Both the iPhone 4 and iPhone 7 were registered to
17 the TARGET ACCOUNT at all relevant times. The iPhone 7 was associated with phone
18 number (253) 722-7826.

19 44. That evening, MV1 communicated via Instagram direct messages with his
20 female friend MV3 using the iPhone 4. MV1 stated that during his conversation with
21 MV3 late in the evening of September 9, 2019, he heard vibrations ostensibly emanating
22 from a cell phone (presumably the iPhone 7) elsewhere in the home and, sometime later,
23 CARPENTER called MV1's name. MV1 immediately suspected that his Instagram
24 communications were also appearing on his iPhone 7 and thereby drawing
25 CARPENTER's interest.

26 45. MV1 stated that CARPENTER then entered his room, approached him and
27 demanded the password for MV1's Instagram account, which he provided. Shortly after
28 providing the password, MV3 informed MV1 that she had received an iMessage from

1 MV1's iPhone 7 which read "Send nudes to me, please." MV3 then forwarded a
 2 screenshot of this message to MV1. The message came from one of MV1's accounts that
 3 was linked to the iPhone 7. MV1 stated that he did not send the message as the phone
 4 was in the possession of CARPENTER. MV3 later forwarded MV1 a screenshot from
 5 MV4's cell phone indicating that she too had received a nude pic solicitation from MV1's
 6 iPhone 7. It is believed that this occurred in the early morning hours of September 10,
 7 2018.

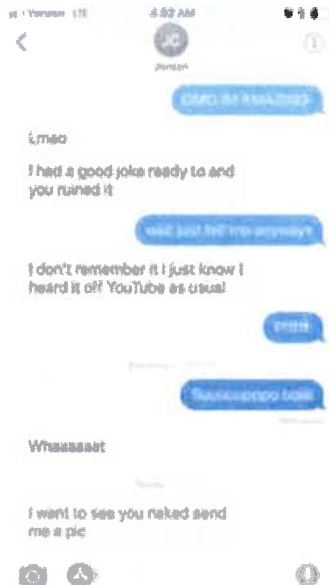
8 46. During her September 17, 2018, interview, Christina Carpenter recalled
 9 MV1 reporting to her that CARPENTER requested the password to MV1's Instagram
 10 account and that CARPENTER utilized MV1's Instagram account on MV1's iPhone 7 to
 11 request nude images from one of MV1's female friends.

12 47. MV3, is a 14-year-old girl currently residing in Kansas with her parents.
 13 During her forensic interview, MV3 indicated that she had been friends with MV1 since
 14 they were students together during the 4th grade in Washington. MV3 confirmed that she
 15 received a message when she was approximately 13-years-old from one of MV1's
 16 Instagram Accounts ("memes_are_pretty_nice") on or about September 10, 2018, while
 17 MV1 was messaging her through another Instagram Account ("silver_cuber"). Such an
 18 occurrence had never happened to her before, which is why she notified MV1 and
 19 forwarded the following screen shot of the solicitation from her phone:



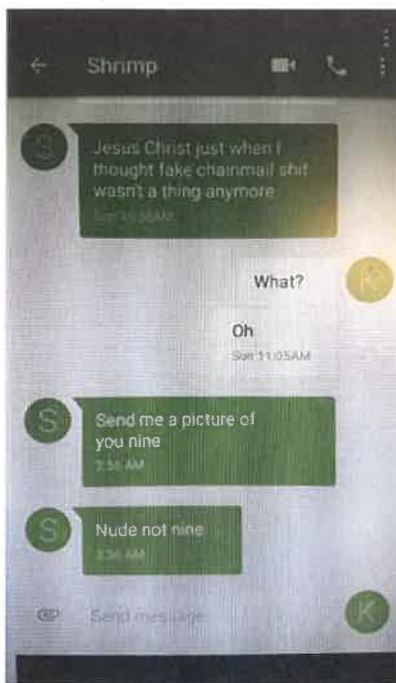
48. MV3 did not provide the requested nude image.

49. In addition to the Instagram request, MV3 also received the following iMessage from MV1's iPhone 7 at approximately 4 a.m. on September 10, 2018:



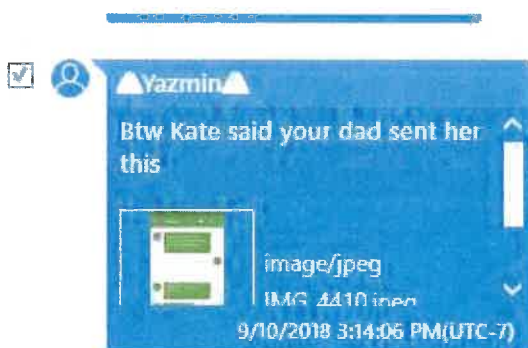
50. As reflected in the extraction report, the iPhone 7 also attempted to FaceTime with MV3 around the same time period.

51. Agents identified a message sent from the iPhone 7 to MV4. On January 17, 2019, agents conducted a forensic interview of MV4 who lived Texas. At the time of the incident, MV4 was 12-years-old and also knew MV1 from elementary school. She specifically received the following message from MV1's iPhone 7 early in the morning on or about September 10, 2018: "[s]end me a picture of you nine...Nude not nine":



52. MV4, realizing that someone must have used MV1's account to make the request, did not produce any images. MV4 discussed the message with MV3. MV3 disclosed to MV4 that she received the same message. MV-3 notified MV1 of the message. A forensic analysis recovered this screen shot.

53. According to the analysis of the iPhone 7, MV3 obtained and forwarded the following copy of CARPENTER's text from MV4 to MV1.



1 54. On January 24, 2019, agents also forensically interviewed MV5, who was
2 12-years-old at the time of the incident and living with her parents in Olympia,
3 Washington. MV5 disclosed that she received a text message from MV1's iPhone 7
4 while she was sleeping sometime in 2018, stating "[p]lease send me nudes." Such a
5 request was unlike any prior messaging that she had received from MV1's phone. MV5
6 did not respond and deleted the message. Law enforcement have not been able to recover
7 the image or record of this message.

8 55. MV1 did not disclose CARPENTER's message to MV5. According to
9 MV5, she did not tell MV1 about her message until sometime later in the fall of 2018 at a
10 large teen social event during which she briefly spoke with MV1.

11 56. On September 5, 2019, FBI SA McNeal interviewed CARPENTER's
12 former spouse, *Christine* Carpenter,² by telephone. While the couple were married in
13 2011, Christine Carpenter described finding sexually explicit videos of children and
14 animals downloaded and saved on CARPENTER's computer when she attempted to
15 check her e-mail and pay bills. She opened up three of the identified videos that were
16 readily accessible on the computer. This incident is believed to have taken place when
17 Christine Carpenter was living near Watertown, New York, while CARPENTER was
18 stationed at Fort Drum as an active duty service member.

19 57. The first video contained apparent bestiality between a horse and an adult
20 female. The second video depicted a nude male child approximately 10-14 years of age
21 sitting and/or standing on a couch while masturbating. Christine Carpenter was asked to
22 describe why she thought the child was 10-14 years of age. Christine Carpenter based
23 her estimate of the child's age on the size of the child's body compared to the size of the
24 couch. Christine Carpenter advised that the video was blurry and that the camera used to
25 take the video was stationary.

26
27
28 ² to be distinguished from his current spouse *Christina* Carpenter.

1 58. The third video depicted a nude Asian female child approximately four to
2 six years of age. The video was approximately five to ten minutes in length. Christine
3 Carpenter described it as an amateur video that was filmed with a handheld camera.
4 During part of the video, the child was lying on the bed, on her back, fully nude.
5 Christine Carpenter described the focal point of the video as the child's vaginal area. The
6 person recording the incident digitally penetrated the child's vagina with his fingers and
7 inserted his penis into the child's vagina. In another part of the video, the female child
8 performed oral sex on the male. Christine Carpenter advised that she did not watch the
9 entire video but just viewed various parts. Christine Carpenter believed the child was
10 four-to-six years of age based on the lack of breast development, absence of pubic hair,
11 and overall body size.

12 59. After viewing the videos, Christine Carpenter searched the computer's
13 browsing history. Christine Carpenter discovered someone, while previously using the
14 computer, had utilized the search terms "6 yr girl" and "Petite girl."

15 60. The following day, Christine Carpenter confronted CARPENTER about the
16 content on his computer and how disgusting she thought it was especially because they
17 had children together. At first, CARPENTER denied searching for the content, stating it
18 just appeared. He initially claimed that it was not his intention to possess the material.

19 61. Later, CARPENTER acknowledged that he was searching the internet for
20 smaller and petite women to which he was attracted. He then admonished Christine
21 Carpenter because, as he argued, people are into different things and, as a result, she
22 should not be critical of his behavior. Christine Carpenter arranged for CARPENTER to
23 speak to her mother, a conversation during which CARPENTER also acknowledged
24 searching the internet for petite women. A subsequent interview of Christine Carpenter's
25 mother indicated that she did remember discovering that CARPENTER had been
26 accessing pornography but did not recall the specific details of the episode.

27 62. As for alcohol, Christine Carpenter related that CARPENTER was a
28 "heavy drinker" and this alcohol use resulted in at least one DUI arrest.

1 63. Christine Carpenter also recalled that CARPENTER routinely ambled
2 through their residence while naked and even asked Christine Carpenter that their
3 wedding be nude-only. CARPENTER acquiesced to a clothed ceremony only after
4 Christine Carpenter's father refused to attend their wedding under these circumstances.
5 Christine Carpenter remembered CARPENTER occasionally fell asleep on the living
6 room couch while naked.

7 64. Finally, Christine Carpenter said CARPENTER's father was convicted and
8 imprisoned for sexually abusing both CARPENTER (at approximately 4 years of age)
9 and his brother. CARPENTER denied that the abuse occurred and instead claimed that
10 his father pled guilty simply to avoid putting his children through the ordeal of a trial.

11 65. On September 17, 2018, FBI Agents and Lacey Police Department Officers
12 contacted CARPENTER at his in Lacey, Washington, and placed him under arrest.

13 66. On September 26, 2018, a federal grand jury presiding in the Western
14 District of Washington returned an Indictment against CARPENTER for committing
15 aggravated sexual abuse of a child under the age of 12 against MV1 and MV2 in
16 violation of 18 U.S.C. §§ 2241(c), 2246(2) and 7.

17 67. On September 25, 2019, a federal grand jury presiding in the Western
18 District of Washington returned a Superseding Indictment against CARPENTER for (1)
19 four counts of committing aggravated sexual abuse of a child under the age of 12 against
20 MV1 and MV2 in violation of 18 U.S.C. §§ 2241(c), 2246(2) and 7 and (2) one count of
21 attempted production of child pornography in violation of 18 U.S.C. §§ 2251(a) and (e).

22 68. CARPENTER is scheduled for trial on May 4, 2020, in cause number 18-
23 CR-5491RJB.

24 69. Based on my training and experience as a Special Agent and the
25 information contained in this Affidavit, I submit there is probable cause to believe that
26 JONATHAN DAVID CARPENTER violated 18 U.S.C. § 2251(a) (Attempted
27 Production of Child Pornography), 18 U.S.C. § 2252(a)(2) (Attempted
28

1 Receipt/Distribution of Child Pornography), and 18 U.S.C. § 2422(b) (Attempted
2 Enticement of a Minor).

3 **VI. INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

4 70. Pursuant to Title 18, United States Code, Section 2703(g), this application
5 and affidavit for a search warrant seeks authorization to permit Apple, and their
6 representatives and employees, to assist agents in the execution of these warrants. Once
7 issued, the search warrants will be presented to Apple with direction that it identify the
8 accounts described in Attachment A, as well as other subscriber and log records
9 associated with the identified account, as set forth in Attachment B.

10 71. The search warrants will direct Apple to create an exact copy of the
11 specified account and records.

12 72. I, and/or other law enforcement personnel will thereafter review the copy of
13 the electronically stored data, and identify from among that content those items that come
14 within the items identified in Section II to Attachment B, for seizure.


15 73. Analyzing the data contained in the forensic image may require special
16 technical skills, equipment, and software. It could also be very time-consuming.
17 Searching by keywords, for example, can yield thousands of “hits,” each of which must
18 then be reviewed in context by the examiner to determine whether the data is within the
19 scope of the warrant. Merely finding a relevant “hit” does not end the review process.
20 Keywords used originally need to be modified continuously, based on interim results.
21 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,
22 search text, and many common e-mail, database and spreadsheet applications do not store
23 data as searchable text. The data may be saved, instead, in proprietary non-text format.
24 And, as the volume of storage allotted by service providers increases, the time it takes to
25 properly analyze recovered data increases, as well. Consistent with the foregoing,
26 searching the recovered data for the information subject to seizure pursuant to this
27 warrant may require a range of data analysis techniques and may take weeks or even
28 months. All forensic analysis of the data will employ only those search protocols and

1 methodologies reasonably designed to identify and seize the items identified in Section II
2 of Attachment B to the warrant.

3 74. Based on my experience and training, and the experience and training of
4 other agents with whom I have communicated, it is necessary to review and seize a
5 variety of messenger communications, chat logs, files, payment records and documents,
6 that identify any users of the specified accounts and communications sent or received in
7 temporal proximity to incriminating messages that provide context to the incriminating
8 communications.

9 **VII. CONCLUSION**

10 75. Based on the information set forth herein, there is probable cause to search
11 the above described **Target Account** and as further described in Attachment A, for
12 evidence, fruits and instrumentalities, as further described in Attachment B, of crimes
13 committed by CARPENTER, specifically Attempted Production of Child Pornography,
14 in violation of 18 U.S.C. § 2251(a) and (e), Attempted Receipt/Distribution of Child
15 Pornography in violation of 18 U.S.C. § 2252(a)(2), and Attempted Enticement of a
16 Minor in violation of 18 U.S.C. § 2422(b).

17
18
19 
20 KYLE MCNEAL
21 Special Agent
22 Federal Bureau of Investigation

23 The above-named agent provided a sworn statement attesting to the truth of the
24 contents of the foregoing affidavit on the 25th day of November, 2019.

25
26 
27 DAVID W. CHRISTEL
28 United States Magistrate Judge